# HOUSE OF REPRESENTATIVES STAFF ANALYSIS

**BILL #:** HB 7157 PCB EDTB 06-03 Internet Phishing
**SPONSOR(S):** Economic Development, Trade & Banking Committee; Bilivakis
**TIED BILLS:** None **IDEN./SIM. BILLS:** None

| REFERENCE | ACTION | ANALYST | STAFF DIRECTOR |
|---|---|---|---|
| Orig. Comm.: Economic Development, Trade & Banking Committee | 13 Y, 0 N | Olmedillo | Carlson |
| 1) Civil Justice Committee | 7 Y, 0 N | Blalock | Bond |
| 2) Criminal Justice Appropriations Committee | | | |
| 3) Commerce Council | | | |
| 4) | | | |
| 5) | | | |

## SUMMARY ANALYSIS


"Phishing" refers to obtaining personal identifying information from individuals via the Internet with the intent to possess or use such information fraudulently.

This bill creates the "Anti-Phishing Act" and will prohibit the acquisition of personal identifying information from a Florida resident through the use of a website or e-mail with the intent to possess or use such information fraudulently. To accomplish this goal the Anti-Phishing Act provides the following:

- Creates a civil cause of action for Internet access providers, financial institutions, web page or trademark owners harmed by a violation, and the Attorney General.
- Provides the plaintiffs with the power to seek injunctive relief and damages in the greater amount of the actual damages arising from the violation, or $5,000 for each violation of the same nature. A court may increase damages to three times the actual damages sustained if violations constitute a pattern. The bill does not preclude the award of damages otherwise available under federal or state law.
- Provides for an award of attorney's fees and costs to a prevailing plaintiff.
- Establishes personal jurisdiction for a violator, sets venue in any county where the plaintiff resides or where any part of the action occurred, and creates a three year statute of limitations.
- Provides that certain moneys received by the Attorney General shall be deposited in the Legal Affairs Revolving Trust Fund.
- Grants the Department of Legal Affairs (Department) rulemaking authority to implement the provisions of this act.

This bill appears to have an indeterminate increased fiscal impact on state revenues and an indeterminate increased fiscal impact on state expenditures. This bill does not appear to have a fiscal impact on local government.

## FULL ANALYSIS

## I. SUBSTANTIVE ANALYSIS

A. HOUSE PRINCIPLES ANALYSIS:

Promote personal responsibility -- This bill increases personal accountability for unlawful actions and injurious behavior.

Provide limited government -- This bill creates a new civil cause of action designed to deter and punish identity theft.

B. EFFECT OF PROPOSED CHANGES:

**Present Situation**

Identity theft is a substantial problem in the United States and “phishing” represents the cutting edge of this devious practice.

“Phishing” refers to obtaining personal identifying information from individuals via the Internet with the intent to possess or use such information fraudulently. Typically, a person attempting to obtain information sends an e-mail that appears to come from a bank or other trusted business requesting an individual to verify their account by typing personal identifying information, such as credit card information, social security numbers, account usernames, passwords, etc. A person may also use a phony web site to trick citizens into forfeiting sensitive personal information.

The Federal Trade Commission (FTC) reported that 27.3 million Americans have been victims of identity theft in the last five years, including 9.9 million people in 2003 alone.[1] According to the FTC, last year’s identity theft losses to businesses and financial institutions totaled nearly $48 billion and consumer victims reported $5 billion in out-of-pocket expenses.[2]

Moreover, according to the Anti-Phishing Working Group, the volume of fraudulent phishing e-mail is growing at a rate in excess of 30 percent each month.[3]

<u>Anti-Phishing Bills in Congress</u>

The Subcommittee on Crime, Terrorism, and Homeland Security of the U.S. House of Representatives is currently reviewing H.R. 1099, which criminalizes internet scams involving the fraudulent obtaining of information, commonly known as “phishing”.[4]

H.R. 1099 imposes a fine or imprisonment for up to five years, or both, for a person who knowingly and with the intent to engage in an activity constituting fraud or identity theft under Federal or State law: (1) creates or procures the creation of a website or domain name that represents itself as a legitimate online business without the authority or approval of the registered owner of such business; and (2) uses that website or domain name to solicit means of identification from any person.

---

[1] See article issued by Federal Trade Commission, dated September 3, 2003 “FTC Releases Survey of Identity Theft in U.S. 27.3 Million Victims in Past 5 Years, Billions in Losses for Businesses and Consumers”. See also http://www.ftc.gov/opa/2003/idtheft.htm.
[2] Id.
[3] The Anti-Phishing Working Group (APWG) is a global pan-industrial and law enforcement association that focuses on eliminating fraud and identity theft that results from phishing and e-mail spoofing of all types.
[4] The Senate companion, S.472 is before the Judiciary Committee.

In addition, H.R. 1099 imposes a fine or imprisonment for up to five years, or both, for a person who knowingly and with the intent to engage in activity constituting fraud or identity theft under Federal or State law sends an electronic mail message that: (1) falsely represents itself as being sent by a legitimate online business; (2) includes an Internet location tool referring or linking users to an online location on the World Wide Web that falsely purports to belong to or be associated with a legitimate online business; and (3) solicits means of identification from the recipient.

**Effect of bill**

Name

This bill creates the "Anti-Phishing Act".

Prohibited Acts

This bill prohibits obtaining identifying information from individuals through certain means via the Internet with the intent to possess or use such information fraudulently. This bill prohibits:

- Representing oneself, either directly or by implication to be another person, without the authority or approval of such other person, through the use of a web page or Internet domain name; and
- Using that web page, a link to the web page, or another site on the Internet to induce, request, or solicit another person to provide identifying information.

This bill also prohibits sending or causing to be sent an e-mail to a resident of this state that:

- Is falsely represented as being sent by another person, without the authority or approval of such other person;
- Refers or links the recipient to a falsely represented web site; and
- Directly or indirectly solicits from the recipient identifying information for a purpose that the recipient believed to be legitimate.

This bill defines or incorporates by reference definitions of terms as follows:

- "Department" means the Department of Legal Affairs.
- "Electronic mail message" means an electronic message or computer file that is transmitted between two or more telecommunications devices; computers; computer networks, regardless of whether the network is a local, regional, or global network; or electronic devices capable of receiving electronic messages, regardless of whether the message is converted to hard copy format after receipt, viewed upon transmission, or stored for later retrieval.[5]
- "Electronic mail address" means a destination, commonly expressed as a string of characters, to which electronic mail may be sent or delivered.[6]
- "Identifying information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any:
    - Name, postal or electronic mail address, telephone number, social security number, date of birth, mother's maiden name, official state-issued or United States-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, Medicaid or food stamp account number, bank account number, credit or debit card number, or personal identification number or code assigned to the holder of a debit card by the issuer to permit authorized electronic use of such card;

[5] s. 668.602(7), F.S.
[6] s. 668.602(6), F.S.

- Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- Unique electronic identification number, address, or routing code;
- Medical records;
- Telecommunication identifying information or access device; or
- Other number or information that can be used to access a person's financial resources.[7]

- "Internet domain name" means a globally unique, hierarchical reference to an Internet host or service, which is assigned through centralized Internet naming authorities and which is comprised of a series of character strings separated by periods, with the right-most string specifying the top of the hierarchy.[8]
- "Web page" means a location that has a single uniform resource locator (URL) with respect to the world wide web or another location that can be accessed on the Internet.

Remedies

This bill gives standing to bring a civil action under this part to:

- A person engaged in the business of providing Internet access to the public who was adversely affected by the violation;
- A financial institution as defined by s. 655.005(1)(h), F.S., adversely affected by the violation.
- An owner of a web page or trademark who was harmed by a violation under this bill; and
- The Attorney General.

A person bringing an action may seek injunctive relief to halt a violation under this bill, recover damages in the greater amount of the actual damages arising from the violation, or $5,000 for each violation of the same nature, or seek both injunctive relief and damages. Violations are considered of the same nature if they consisted of the same action or course of conduct regardless of how many times the act occurred. A court may increase damages to three times the actual damages sustained if violations constitute a pattern or practice.

This bill also provides for an award of attorney's fees and costs to a prevailing plaintiff.

This bill provides that the violator submits personally to the jurisdiction of the courts of the State of Florida by committing a violation of this Act. In addition, the bill establishes a 3 year statute of limitations to bring a suit under the Act.

This bill also provides that venue lies in any county in which the plaintiff resides or in which any part of the violation occurred.

This bill requires that any moneys received by the Attorney General for attorney's fees and costs, or not utilized to reimburse persons harmed under this act, shall be deposited in the Legal Affairs Revolving Trust Fund.

This bill does not preclude the award of damages otherwise available for the same conduct pursuant to federal or state law.

This bill grants the Department rulemaking authority to implement the provisions of this act.

Exemption

[7] s. 817.568(1)(f), F.S.
[8] s. 668.602(10), F.S.

This bill exempts from liability a telecommunication provider's or an Internet service provider's good faith transmission or intermediate temporary storing of identifying information. The bill also exempts providers of an interactive computer service when removing or disabling access to content that resides on an Internet website or other online location controlled or operated by such provider if such provider believes in good faith that the content is used to engage in a violation of the provisions of this bill.

C. SECTION DIRECTORY:

Section 1 creates s. 668.701, F.S., to provide a title; s. 668.702, F.S., to provide definitions; s. 668.703, F.S., to provide prohibited acts; s. 668.704, F.S., to provide remedies and standing; and s. 668.705, F.S., to provide exemptions.

Section 2 provides an effective date of October 1, 2006.

## II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   See Fiscal Comments.

2. Expenditures:

   See Fiscal Comments.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

   None.

2. Expenditures:

   None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

This bill also provides that the Attorney General may bring a civil action against a person that violates the Act, and would be able to collect the greater of the actual damages or $5,000, which is to be deposited into the Legal Affairs Revolving Trust Fund.

The bill grants the Attorney General authority to enforce violations under this bill. Therefore, the Attorney General will incur costs in order to prosecute persons that violate this bill. The costs, however, are indeterminate.

According to the Department of Legal Affairs, it prosecuted only two cases under the 2004 Electronic Mail Communications Act, which creates criminal penalties for sending unsolicited false or misleading commercial electronic mail messages to an electronic mail address that is held by a resident of Florida. A number of persons filed additional complaints; however the Department of Legal Affairs has not been able to determine who sent the messages, preventing further action under the statute.

## III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

This bill does not appear to require counties or municipalities to take an action requiring the expenditure of funds, reduce the authority that counties or municipalities have to raise revenue in the aggregate, nor reduce the percentage of state tax shared with counties or municipalities.

2. Other:

This Act creates sections 668.701 – 668.705, F.S., to provide civil penalties for the acquisition of personal identifying information from a resident of this State with the intent to possess or use such information fraudulently. Under certain circumstances, it is possible that this bill could assert Florida's police power over non-residents of Florida, and therefore this bill could possibly violate the Commerce Clause of the U.S. Constitution.

The Commerce Clause empowers Congress to regulate commerce among the several states.[9] "This affirmative grant of authority to Congress also encompasses an implicit or dormant limitation on the authority of the States to enact legislation affecting interstate commerce."[10] The aspect of the Commerce Clause, which operates as an implied limitation upon state and local government authority is often referred to as the dormant Commerce Clause.[11]

In Pike v. Bruce Church Inc.,[12] the court devised a two prong test to determine if a state statute violates the dormant Commerce Clause:

> Where the statute regulates even-handedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits. If a legitimate local purpose is found, then the question becomes one of degree. And the extent of the burden that will be tolerated will of course depend on the nature of the local interest involved, and on whether it could be promoted as well with a lesser impact on interstate activities.

The Supreme Court explained that the critical consideration is the overall effect of the statute on both local and interstate activity with respect to both parts of the Pike test.[13] The Supreme Court has invalidated statutes under the Pike test on the grounds that their extraterritorial effect renders them unconstitutional.

For instance, in Healy, the court held:

> [T]he extraterritorial effects of state economic regulation stand at a minimum for the following proposition:
>
> First, the "commerce clause . . . preludes the application of a state statute to commerce that takes place wholly outside of the State's borders, whether or not the commerce has effects within the State" . . . . Second, a statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State's authority and is invalid regardless of whether the statute's extraterritorial reach was intended by the legislature. The critical inquiry is whether the practical effect of the regulation is to control conduct beyond the boundaries of the State. Third, the practical effect of the statute must be evaluated not only by considering the consequences of the statute itself, but also by considering how the challenged statute may interact with the legitimate regulatory regimes of other Sates and what effect would arise if not one, but

[9] *See* U.S. Const., art. I, § 8, cl. 3.
[10] Healy v. The Beer Insitiute, 491 U.S. 324 (1989).
[11] MaryCle, LLC. v. First Choice Internet, Inc., 2006 WL 173659 (Md. App. 2006); citing Bd. of Trs. of the Employees' Ret. Sys. of Baltimore City v. Mayor and City Council of Baltimore, 317 Md. 72 at 131 (1989).
[12] 397 U.S. 137 (1970).
[13] *See* Brown-Forman Distillers Corp. v. N.Y. State Liquor Authority, 476 U.S. 573 at 579 (1986).

> many or every, State adopted similar legislation. Generally speaking, the Commerce Clause protects against inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another state.[14]

In American Libraries Ass'n v. Pataki[15], the first case to apply the dormant Commerce Clause to a state law on Internet use[16], a federal trial court granted an injunction preventing the State of New York from enforcing a statute that criminalized intentional communications via the internet for the purpose of engaging in harmful sexual conduct with a minor. The court held that the New York Act is concerned with interstate commerce and contravenes the Commerce Clause for three reasons:

> First, the Act represents an unconstitutional projection of New York law into conduct that occurs wholly outside New York. Second, the Act is invalid because although protecting children from indecent material is a legitimate and indisputably worthy subject of state legislation, the burdens on interstate commerce resulting from the Act clearly exceed any local benefit derived from it. Finally, the Internet is one of those areas of commerce that must be marked off as a national preserve to protect users from inconsistent legislation that, taken to its most extreme, could paralyze development of the Internet altogether. Thus, the Commerce Clause ordains that only Congress can legislate in this area, subject, of course, to whatever limitations other provisions of the Constitution (such as the First Amendment) may require.[17]

"Many courts have followed the logic of American Libraries Ass'n."[18]

Moreover, courts have examined "spam" statutes, which prohibit unsolicited false or misleading commercial electronic mail under the dormant Commerce Clause and found those statutes to be constitutional.[19]

In Heckel, the court held that there was no sweeping extraterritorial effect that would outweigh the local benefits of the Act because the statute regulates only those emails directed to a Washington resident or sent from a computer located within Washington.[20] The Act specifically prohibited e-mail solicitors from using misleading information in the subject line or transmission path of any commercial e-mail message sent to Washington residents or from a computer located in Washington.[21] The court distinguished the case from American Libraries Ass'n stating that the Washington Act did not impose liability for messages that are merely routed through Washington or that are read by a Washington resident who was not the actual addressee.[22]

In MaryCle, the court held that a Maryland statute was facially neutral because it applies to all email advertisers, regardless of their geographic location. It does not discriminate against out-of-state senders.[23]

In Ferguson, the court held that a California statute did not violate the commerce clause because the only burden on interstate commerce is that the email be truthful and non-deceptive email.[24]

---

[14] Healy at 336-37; *see also* MaryCle, at 15.
[15] Am. Libraries Ass'n, 969 F. Supp. 160 (S.D.N.Y. 1997).
[16] *See* State v. Heckel, 24 P.3d 404 (Wash 2001).
[17] Am. Libraries Ass'n, 969 F. Supp. at 169 (S.D.N.Y. 1997)
[18] *See* The Internet and the Dormant Commerce Clause, 110 The Yale Law Journal 787 (2001).
[19] *See* State v. Heckel, 24 P.3d 404 (Wash 2001); MaryCle, LLC. v. First Choice Internet, Inc., 2006 WL 173659 (Md. App. 2006); Ferguson v. Friendfinders, Inc., 94 Cal.App.4th 1255 (1st Dist. 2002).
[20] Heckel ,at 412-13.
[21] Id at 413.
[22] Id.
[23] MaryCle, at 19.
[24] Feruson, at 1265.

Similarly, in Cashatt, a Florida court, using the Pike test, upheld a statute that criminalized the use of a computer on-line service or Internet service to seduce, lure or entice, a child to commit any illegal act.[25]

The Anti-Phishing Act, appears to apply evenhandedly to in-state and out-of-state transmitters. The local benefit of this Act is to protect the public and businesses from misleading and deceptive practices involving fraudulent use of personal information, a legitimate local public interest, and the only burden imposed is not using the Internet for the purpose of obtaining another's personal information for a fraudulent purpose.

B. RULE-MAKING AUTHORITY:

The bill grants the Department of Legal Affairs rulemaking authority to implement the provisions of the Act.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

## IV. AMENDMENTS/COMMITTEE SUBSTITUTE & COMBINED BILL CHANGES

On March 16, 2006, the Economic Development, Trade and Banking Committee adopted an amendment to the bill. The amendment adds an exemption for providers of interactive computer services who remove or disable access to content due to a good faith belief that the content is being used to violate provisions of this bill. The bill was then reported favorably with a committee substitute.

[25] *See* Cashatt v. State, 873 So.2d 430 (1st DCA 2004).